RTM GROUP

Информационная безопасность для Банков и НФО: самое важное в 2023 году

RTM GROUP

Объединяем IT,
право и безопасность

Далее

СПИКЕРЫ

Фёдор Музалевский

- **Директор** технического департамента RTM Group
- **Экспертная работа** с 2010 года. Педагогический стаж с 2012 года
- **Кандидат** физико-математических наук.
- **Участник ТК №122** при Банке России.

Дмитрий Кобец

- **Заместитель директора** технического Департамента
- **Эксперт** в сфере информационной безопасности
- **Профессиональный опыт** в сфере ИТ и информационной безопасности с 2009 года
- **Участник ТК №122** при Банке России.

О КОМПАНИИ RTM GROUP

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Информационная безопасность:

Аудиты, пентест, КИИ, защита ПДн, оценка защищённости и др.

Компьютерно-технические экспертизы:

44-ФЗ, расследования инцидентов, ИТ-контракты и др.

ИТ-право:

Судебное и досудебное урегулирование, сопровождение и др.

ПРОГРАММА

01 **Краткий обзор и сроки:**

- Положений и требований ЦБ по ИБ
- Положений по киберрискам и опернадежности
- Отчетности перед ЦБ (форма 0409071 и 0409106)
- Сопутствующих требований по ОУД4 и пентесту
- Прочих требования законодательства

02 **Рекомендации** по экономии бюджетов.

03 **Ответы** на ваши вопросы.

ОБЗОР ПОЛОЖЕНИЙ И РАЗБОР СРОКОВ ИСПОЛНЕНИЯ

01

Положение № 683-П

683-П

С 1 января 2023

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка по ГОСТ: раз в 2 года

Проверяется лицензиатом ФСТЭК

Положение № 719-П

719-П

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка лицензиатом ФСТЭК (п.1.1).

Положение № 802-П

802-П

С 1 января 2023

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка не реже одного раза в два года (п.20).
ССНП, СБП, ОУИО СБП - стандартный уровень (уровень 2) ГОСТ 57580.
ОПКЦ СБП - усиленный уровень (уровень 1) ГОСТ 57580.

Приказ № 930

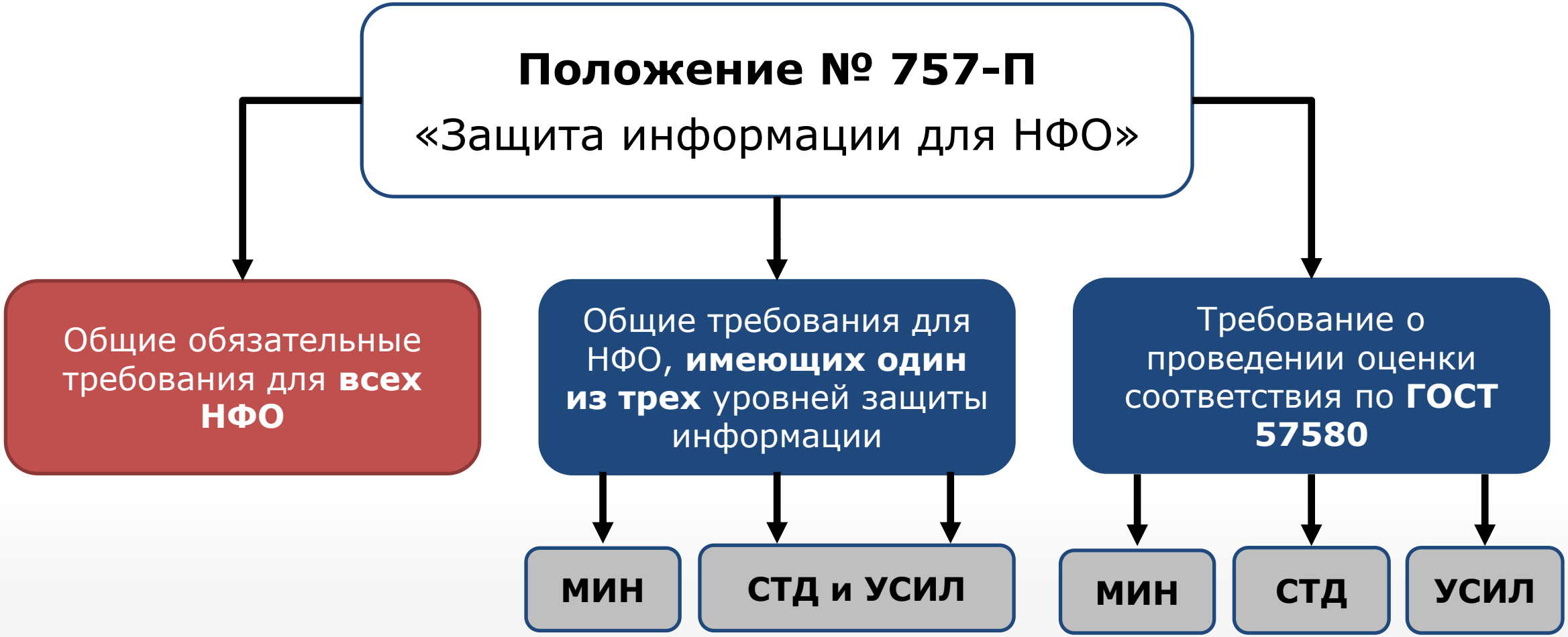
Приказ 930

Ежегодно

Уровень соответствия не указан

Оценка лицензиатом ФСТЭК (п.7 Приложения 1).
Стандартный уровень (уровень 2) ГОСТ 57580 (п.4 Приложения 3).

Положение № 757-П



Общие обязательные требования для **всех НФО**

п.1.2, п.1.3

Защита информации с помощью СКЗИ

п.1.4.1

Ежегодное определение уровня защиты информации не позднее десятого рабочего дня календарного года.

п.1.8

Фиксация решения о применимости оценки соответствия ОУД4

В 757-П НФО могут быть без уровня. ГОСТ 57580 – не применим

Положение № 757-П

757-П

С 1 июля 2023

- Не ниже **четвертого**
- Числовая оценка > 0,85

Оценка по ГОСТ 57580:

- усиленный (1 уровень) раз в год;
- стандартный (2 уровень) раз в 3 года.

Привлечение лицензиатов ФСТЭК (п.1.5.1).

Форма 0409071 и 12-МР

- **Раздел 1.** Сведения об оценке выполнения требований по направлению «Технологические меры»

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

- **Раздел 2.** Сведения об оценке выполнения требований по направлению «Безопасность программного обеспечения»

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

- **Раздел 3.** Сведения об оценке выполнения требований по направлению «Безопасность информационной инфраструктуры»

Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
...					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z					
Итоговая оценка соответствия, R					

- **Раздел 4.** Сведения о проверяющей организации.

С 01.10.2022 г. один раз в два года

Положение № 716-П

Положение Банка России от 8 апреля 2020 г.
№ 716-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

ЦБ РФ данным положением: установил требования к системе управления операционным риском в кредитной организации и банковской группе. Приведен классификатор событий. Уточнены способы управления.

Привлечение внешней организации не требуется.

Форма 0409102.
Отчет по управлению операционным риском в кредитной организации

1. **Заполняются** 3 раздела, включая подразделы
2. **ЦБ** предлагает форму в MS-Excel

С 01.10.2022

Ежеквартальная

Положение № 787-П

Положение от 12 января 2022 года
№ 787-П
«Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»

Данным положением ЦБ установил требования к разработке документов по операционной надежности, а также пороговые значения допустимого времени простоя и (или) деградации технологических процессов.

Привлечение внешней организации не требуется.

Положение № 779-П

Положение от 15 ноября 2021 года
№ 779-П
«Об установлении обязательных для некредитных финансовых организаций требованиях к операционной надежности при осуществлении видов деятельности в целях обеспечения непрерывности оказания финансовых услуг»

Данным положением ЦБ установил требования к разработке документов по операционной надежности, а также пороговые значения допустимого времени простоя и (или) деградации технологических процессов.

Привлечение внешней организации не требуется.

Положения № 787-П и 779-П

779-П

Срок выполнения

01.10.2022

787-П

Независимая оценка SWIFT

SWIFT

Окно аттестации с 1 июля до 31 декабря

Все пользователи:
независимая внешняя оценка на соответствие требованиям SWIFT Customer Security Program.

Федеральный закон № 152-ФЗ

Федеральный закон
N 152-ФЗ
«О персональных данных»

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Аудит проводится на соответствие требованиям Законодательства.

«Бумажная» безопасность.
Разработка внутренней документации по ПДн.

Что требуется сделать:

1. Разработать и ввести в действие организационно-распорядительную документацию в отношении обработки и защиты ПДн.
2. Провести моделирование угроз.

«Реальная» безопасность.
Обеспечение техническими средствами.

Организации при обработке персональных данных необходимо самостоятельно обеспечить техническими средствами:

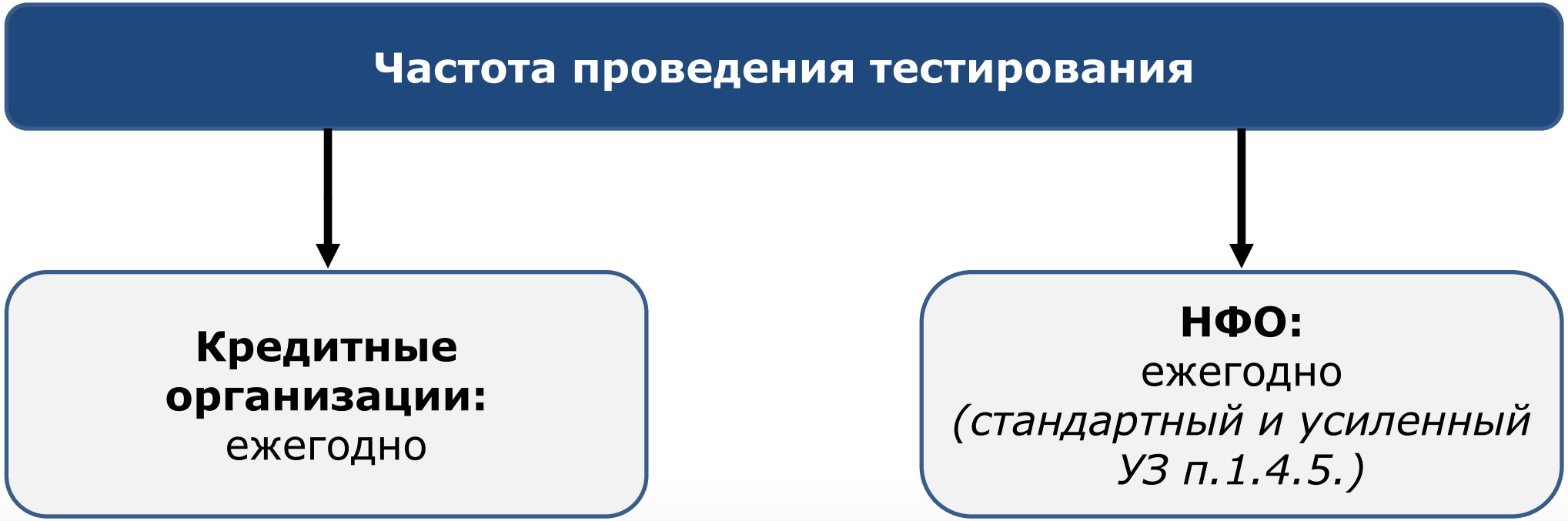
Аутентификация пользователей	Штатные средства ОС как базовый вариант
Физическая защита	Двери, турникеты, видеокамеры, замки и т.д.
Технические средства защиты	Межсетевые экраны, сетевые сканеры, антивирусы, DLP, SIEM и т.д.

Федеральный закон № 187-ФЗ

Федеральный закон от 26 июля 2017 г
«О безопасности критической информационной инфраструктуры Российской Федерации

187-ФЗ	Категорирование объектов КИИ

Пентест.
Тестирование на проникновение и анализ уязвимостей



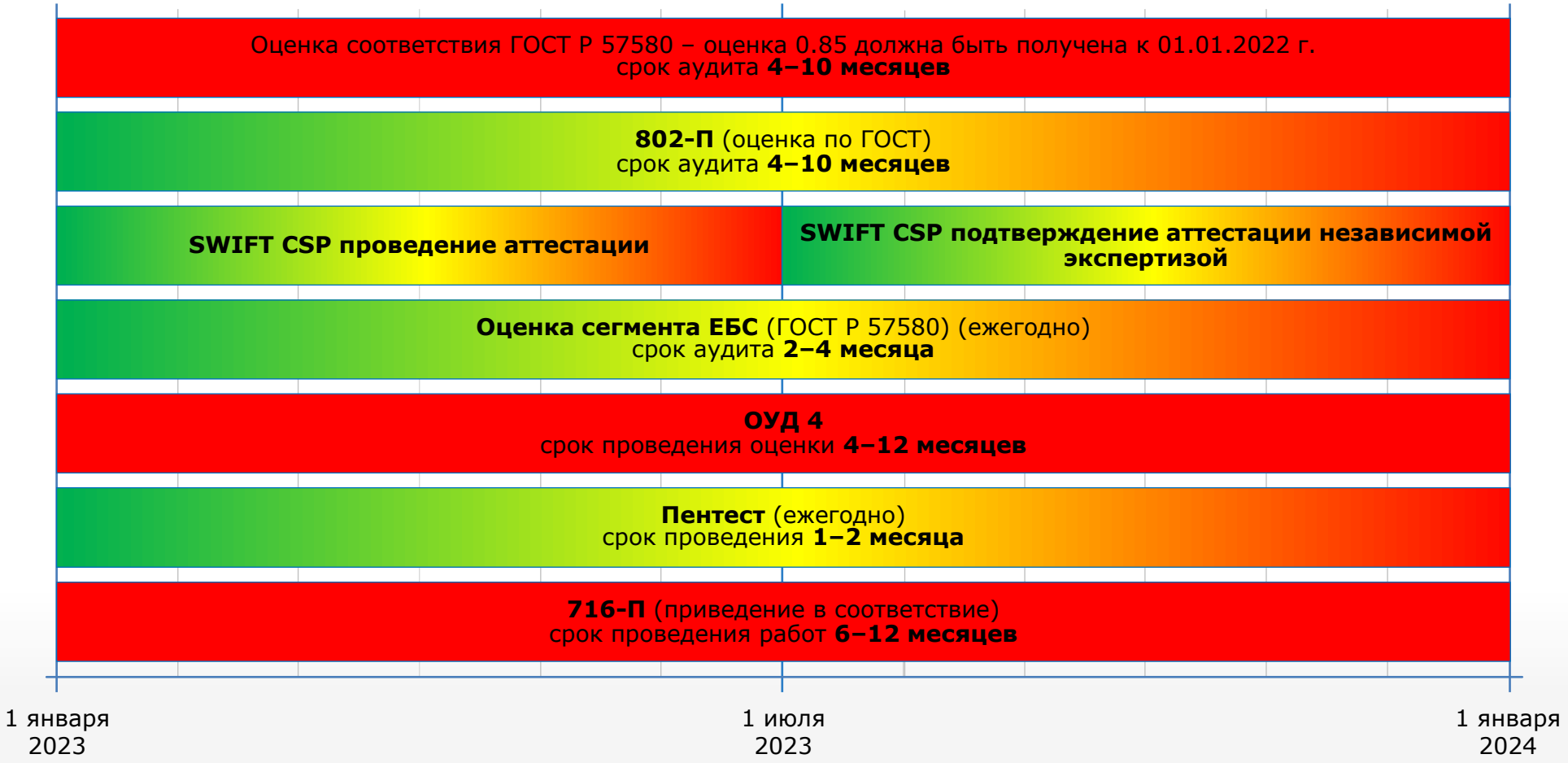
Оценка соответствия ПО (ОУД4)

Проведение оценки соответствия

- **683-П**
- **719-П**
- **757-П п.1.8.** (стандартный и усиленный уровень)

Анализ проводится при каждой смене версии ПО.

Сроки исполнения положений



РЕКОМЕНДАЦИИ ПО ОПТИМИЗАЦИИ БЮДЖЕТА

Как выполнить все требования ЦБ
и уменьшить на это затраты денежных средств?

02

Оптимизация: 4 аудита в 1

Одним аудитом – можно!
Письмо ЦБ № 56-1-11/265 от 22.05.2020 г.

* - *при совмещении деятельности НФО*

Оптимизация своими силами

Тестирование на проникновение

Оценка соответствия ОУД 4

Разработка ОРД

Поддержка банков в спорах по хищениям денежных средств

Экспертиза ДБО на предмет соблюдения требований законодательства

Анализ обстоятельств хищения на предмет нарушения условий договора с клиентом

Консультирование и представительство в судах

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Музалевский Федор Александрович

Директор технического департамента RTM Group

Ведущий судебный эксперт

Кобец Дмитрий Андреевич

Замдиректора техдепартамента RTM Group

Эксперт в сфере информационной безопасности

 +7(495)197-64-95

 info@rtmtech.ru

 https://rtmtech.ru

 rtm.group

 t.me/kurilka_ib